Microsoft Security

ดัชนีความปลอดภัยของข้อมูล

แนวโน้ม ข้อมูลเชิงลึก และกลยุทธ์เพื่อรักษาข้อมูลของคุณให้ปลอดภัย
และนำทาง generative AI

รายงานประจำปี 2024

คำนำ

ขณะที่เราเริ่มปีที่สองของการวิจัยเกี่ยวกับภูมิทัศน์ด้านความปลอดภัยของข้อมูลที่เปลี่ยนแปลงตลอดเวลา ความท้าทายและโอกาสเบื้องหน้าเราไม่เคยลึกล้ำเท่านี้มาก่อน ในปีที่ผ่านมา เหตุการณ์ด้านความปลอดภัยของข้อมูลมีความรุนแรงมากขึ้น ในยุคที่เน้นการใช้ข้อมูลเป็นหลักนี้ กลยุทธ์และเครื่องมือที่ใช้ในการปกป้องข้อมูลมีการพัฒนาอย่างรวดเร็ว

ปีนี้เราจะสำรวจขอบเขตใหม่: บทบาทและผลกระทบของ generative AI (AI) ต่อกลยุทธ์การรักษาความปลอดภัยข้อมูล

AI กำลังสร้างกระแสทั่วโลกด้วยความสามารถที่ไม่เคยมีมาก่อนเพื่อปลดล็อกนวัตกรรมและประสิทธิภาพที่เพิ่มขึ้น แต่ด้วยศักยภาพมหาศาลนี้ องค์กรต่างๆ ยังคงกังวลกับความเสี่ยงด้านความปลอดภัยของข้อมูล และกังวลว่าศักยภาพดังกล่าวจะกำหนดความรับผิดชอบสำหรับทีมรักษาความปลอดภัยข้อมูลอย่างไร เรามองว่า AI เป็นตัวเร่งให้องค์กรเสริมสร้างแนวทางปฏิบัติด้านความปลอดภัยของข้อมูลพื้นฐานเพื่อให้พวกเขาสามารถเตรียมพร้อมเพื่อลดผลกระทบของการแชร์ข้อมูลมากเกินไปและการรั่วไหลของข้อมูล และสร้างกระบวนการสำหรับการนำ AI มาใช้อย่างปลอดภัย ในทางกลับกัน AI ยังสามารถช่วยองค์กรปรับปรุงแนวทางปฏิบัติด้านความปลอดภัยของข้อมูลโดยระบุความเสี่ยงและช่องว่างในการป้องกันที่แอบแฝงอยู่ การแนะนำนโยบายป้องกันตลอดจนช่วยตรวจสอบและแก้ไขเหตุการณ์ด้านความปลอดภัยได้เร็วขึ้น

เป้าหมายการวิจัยของเราคือการให้ข้อมูลเชิงลึกและคำแนะนำที่นำไปปฏิบัติได้แก่ผู้นำด้านความปลอดภัยของข้อมูลเพื่อช่วยให้ทีมของพวกเขาปรับกลยุทธ์การรักษาความปลอดภัยข้อมูลได้อย่างมั่นใจเพื่อปกป้องการใช้ AI รวมถึงการผสานรวม AI ในกลยุทธ์การรักษาความปลอดภัยข้อมูล แม้มีความโดดเด่นในด้านการเข้าถึงและศักยภาพ แต่ AI เป็นเพียงคลื่นแห่งการเปลี่ยนแปลงล่าสุดที่ครอบคลุมทั่วทั้งองค์กร เช่น การทำงานแบบไฮบริด ระบบคลาวด์ และระบบเคลื่อนที่ ซึ่งในช่วงหลายปีที่ผ่านมาได้ตอกย้ำความจำเป็นที่ไร้กาลเวลาของความสามารถในการมองเห็นในการใช้งานเพื่อลดความเสี่ยงและเพิ่มผลกระทบสูงสุด ด้วยการเรียนรู้เหล่านี้ การรักษาความปลอดภัยข้อมูลที่ใช้ใน AI อย่างเหมาะสม รวมถึงการใช้ AI เพื่อปรับปรุงมาตรการรักษาปลอดภัยข้อมูลจะช่วยเพิ่มประสิทธิภาพการทำงาน ความยืดหยุ่น และความคล่องตัวเมื่อทีมทำการสำรวจความท้าทายในอนาคต

เราขอเชิญให้คุณสำรวจผลการค้นพบล่าสุดและหวังว่าข้อมูลเชิงลึกจะช่วยให้คุณเสริมสร้างมาตรการรักษาความปลอดภัยข้อมูลของคุณ รวมถึงสร้างแรงบันดาลใจให้คุณเปิดรับ AI และสร้างกลยุทธ์การรักษาความปลอดภัยข้อมูลที่ครอบคลุม ปลดล็อกนวัตกรรมเพิ่มเติม และสร้างอนาคตที่ปลอดภัยมากขึ้นสำหรับเราทุกคน

Rudra Mitra
รองประธานบริษัท
ความปลอดภัยของข้อมูลและการปฏิบัติตามข้อบังคับของ Microsoft

ข้อมูลเบื้องต้น

ขณะที่องค์กรเผชิญเหตุการณ์ด้านความปลอดภัยของข้อมูลเฉลี่ย 156 ครั้งต่อปี ผลกระทบของเหตุการณ์เหล่านี้ยังคงเป็นข้อกังวลอย่างต่อเนื่องสำหรับผู้มีอำนาจตัดสินใจด้านความปลอดภัยของข้อมูล เหตุผลที่อธิบายเรื่องนี้ได้เป็นอย่างดีคือ เหตุการณ์เดียวอาจทำให้เกิดความเสียหายทางการเงินและชื่อเสียงอย่างรุนแรง โดยเฉพาะอย่างยิ่งในภูมิทัศน์ที่ภัยคุกคามเปลี่ยนแปลงตลอดเวลา ซึ่งผู้โจมตีกำลังใช้ประโยชน์จากช่องโหว่ที่เป็นไปได้ทั้งหมด ความเสียหายนี้รังแต่จะเพิ่มขึ้นจากการนำ AI มาใช้อย่างรวดเร็ว ซึ่งหากไม่มีการป้องกันและมาตรการรักษาความปลอดภัยที่เพียงพอ ผู้ใช้อาจทำให้ข้อมูลทางธุรกิจที่ละเอียดอ่อน (รวมถึงข้อมูลพนักงานและข้อมูลลูกค้า ทรัพย์สินทางปัญญา การคาดการณ์ทางการเงิน และข้อมูลการดำเนินงาน) ตกอยู่ในความเสี่ยงโดยไม่ตั้งใจหรือโดยมีเจตนาร้าย ขณะที่องค์กรมองหาวิธีใหม่ๆ ในการปกป้องข้อมูลที่ละเอียดอ่อนและหลากหลายนี้ ผู้มีอำนาจตัดสินใจจำนวนมากจึงหันมาสนใจการเติบโตอย่างชัดเจนของ AI

ความท้าทายของ AI เพิ่มขึ้นเป็นสองเท่า เนื่องจาก 2 ใน 3 ขององค์กรยอมรับว่าพนักงานกำลังใช้เครื่องมือ AI ที่ไม่ได้รับอนุญาต องค์กรเหล่านั้นจึงต้องมั่นใจว่าพนักงานใช้เครื่องมือ AI อย่างปลอดภัย ขณะเดียวกันมีโอกาสที่จะใช้ AI เป็นเครื่องมือที่มีประสิทธิภาพในกลยุทธ์การรักษาความปลอดภัยข้อมูลที่ซับซ้อน

โซลูชันการรักษาความปลอดภัยข้อมูลที่ขับเคลื่อนด้วย AI มีบทบาทสำคัญในการระบุและตอบสนองต่อภัยคุกคามในเวลาจริง การปรับปรุงความเร็วและความเที่ยงตรงโดยรวมของโปรแกรมการรักษาความปลอดภัยข้อมูล และการให้ข้อมูลเชิงลึกที่ช่วยป้องกันเหตุการณ์ด้านความปลอดภัยของข้อมูลก่อนที่จะเกิดขึ้น องค์กรต้องจัดการความเสี่ยงที่เกิดจาก AI นอกเหนือจากการควบคุมความสามารถของ AI เพื่อระบุรูปแบบที่อาจท้าทายมนุษย์ในการประมวลผลและวิเคราะห์ที่ระดับความเร็วของเครื่อง และต่อสู้กับการโจมตีทางไซเบอร์ที่มีความซับซ้อนมากขึ้นในท้ายที่สุด

ในปี 2023 Microsoft มอบหมายให้ Hypothesis ซึ่งเป็นหน่วยงานวิจัยอิสระ ดำเนินการสำรวจความคิดเห็นผู้เชี่ยวชาญด้านความปลอดภัยของข้อมูลกว่า 800 คนในประเทศต่างๆ และเริ่มดำเนินการแนวคิดริเริ่มเกี่ยวกับดัชนีความปลอดภัยของข้อมูลเพื่อให้บริการคู่ค้าและลูกค้าของเราได้ดียิ่งขึ้น และช่วยให้ผู้นำธุรกิจพัฒนากลยุทธ์การรักษาความปลอดภัยข้อมูลของตนเอง

ในปี 2024 รายงานฉบับนี้ถูกสร้างขึ้นจากงานวิจัยก่อนหน้านี้พร้อมข้อมูลเชิงลึกใหม่ๆ จากการสำรวจความคิดเห็นที่ขยายเพิ่มเติมครอบคลุมผู้เชี่ยวชาญด้านความปลอดภัยของข้อมูลกว่า 1,300 คนจากหลายประเทศ แม้ข้อมูลเผยให้เห็นข้อมูลเชิงลึกและแนวโน้มที่สอดคล้องกันในตลาดที่เราทำการสำรวจ แต่เรายังค้นพบการเรียนรู้ใหม่ๆ เกี่ยวกับความปลอดภัยของข้อมูลล่าสุด และแนวทางปฏิบัติและแนวโน้มของ AI ทั่วโลก

ประเด็นสำคัญ

1

ภูมิทัศน์ด้านความปลอดภัยของข้อมูลยังคงกระจัดกระจาย ทำให้กลยุทธ์การรักษาความปลอดภัยข้อมูลที่สอดคล้องสำหรับความเสี่ยงทั้งแบบดั้งเดิมและที่เกิดขึ้นใหม่ที่เชื่อมโยงกับการใช้ AI มีความจำเป็นมากขึ้น

องค์กรรายงานว่ามีความพึงพอใจและความมั่นใจในมาตรการรักษาความปลอดภัยข้อมูลของตนในระดับสูง อย่างไรก็ตาม เหตุการณ์ด้านความปลอดภัยของข้อมูลยังคงมีความรุนแรงมากขึ้น โดยเฉพาะอย่างยิ่งเนื่องจากช่องว่างที่องค์กรพบระหว่างนโยบายความปลอดภัยของข้อมูลในปัจจุบันกับการใช้งาน/การแนะนำแอปพลิเคชัน AI ที่เพิ่มขึ้น เมื่อเผชิญเดิมพันและความจำเป็นเหล่านี้ องค์กรหลายแห่งยังคงพึ่งพาเครื่องมือรักษาความปลอดภัยข้อมูลหลายอย่าง ซึ่งอาจส่งผลให้มีช่องโหว่และความเสี่ยงโดยรวมเพิ่มขึ้น

2

การที่ผู้ใช้นำแอป AI มาใช้มากขึ้นส่งผลให้ความสมบูรณ์ของข้อมูลที่ละเอียดอ่อนที่สุดขององค์กรมีความเสี่ยงมากขึ้น ซึ่งต้องการการมองเห็นและการควบคุมการป้องกันใหม่ๆ มากขึ้น

เนื่องจากเครื่องมือ AI กลายเป็นสิ่งจำเป็นต่อการทำงานประจำวัน องค์กรจึงกังวลเกี่ยวกับความเสี่ยงด้านความปลอดภัยของข้อมูล พวกเขาตระหนักถึงความจำเป็นในการเสริมสร้างการป้องกันและมุ่งมั่นที่จะป้องกันเหตุการณ์ด้านความปลอดภัยของข้อมูลที่เกิดจาก AI แต่การใช้เครื่องมือเหล่านี้โดยไม่ได้รับอนุญาตตอกย้ำความจำเป็นของความสามารถในการมองเห็นอย่างมีประสิทธิภาพยิ่งขึ้น

3

ผู้มีอำนาจตัดสินใจมองโลกในแง่ดีเกี่ยวกับศักยภาพของ AI ในการเพิ่มความพยายามด้านความปลอดภัยของข้อมูล

องค์กรกำลังทุนอย่างจริงจังในเครื่องมือรักษาความปลอดภัยข้อมูลที่ผสานรวม AI เพื่อปรับปรุงความสามารถในการตรวจหาและการตอบสนอง AI สามารถช่วยตรวจหาข้อมูลที่ไม่มีการป้องกัน แนะนำนโยบายการป้องกัน และช่วยตรวจสอบและแก้ไขเหตุการณ์ด้านความปลอดภัยของข้อมูลได้เร็วขึ้น ช่วยให้ทีมรักษาความปลอดภัยข้อมูลสามารถทุ่มเทเวลาและความสนใจกับงานเชิงกลยุทธ์มากขึ้น การใช้ AI ยังช่วยเพิ่มความเชื่อมั่นและความพึงพอใจในกลยุทธ์การรักษาความปลอดภัยข้อมูลโดยรวมขององค์กร โดยเฉพาะอย่างยิ่งความสามารถในการตอบสนองต่อเหตุการณ์อย่างรวดเร็วและถูกต้อง

1

ภูมิทัศน์ด้านความปลอดภัยของข้อมูลยังคงกระจัดกระจาย ทำให้กลยุทธ์การรักษาความปลอดภัยข้อมูลที่สอดคล้องสำหรับความเสี่ยงทั้งแบบดั้งเดิมและที่เกิดขึ้นใหม่ที่เชื่อมโยงกับการใช้ AI มีความจำเป็นมากขึ้น

มีความไม่สอดคล้องกันระหว่างความเชื่อมั่นของผู้มีอำนาจตัดสินใจในแนวทางปฏิบัติด้านความปลอดภัยของข้อมูลและระดับการปกป้องข้อมูลที่แท้จริง

ดังที่มีการรายงานในปี 2023 ผู้มีอำนาจตัดสินใจส่วนใหญ่เชื่อมั่นในกลยุทธ์การรักษาความปลอดภัยข้อมูล โดยรายงานว่ามีความพึงพอใจ 74% ต่อโซลูชันในปัจจุบัน ในปี 2024 พวกเขายังรู้สึกมั่นใจกับความสามารถในการติดตามและจัดการข้อมูลที่ละเอียดอ่อน: 88% เชื่อว่าพวกเขารู้ว่าข้อมูลสำคัญส่วนใหญ่อยู่ที่ใด และ 85% ระบุว่าข้อมูลของพวกเขาได้รับการจำแนกและติดป้ายกำกับอย่างถูกต้อง ผู้มีอำนาจตัดสินใจส่วนใหญ่ยังไว้วางใจในการควบคุมการป้องกันของตนเอง โดย 79% เชื่อมั่นว่าสามารถป้องกันการลักลอบถ่ายโอนข้อมูล และ 76% อธิบายว่าแนวทางของตนเองเป็นแนวทางเชิงรุกแทนที่จะเป็นเชิงรับ

อย่างไรก็ตาม ความเชื่อมั่นของพวกเขาจะถูกทดสอบเมื่อความรุนแรงของเหตุการณ์ยังคงเพิ่มขึ้น **โดยเฉลี่ยแล้ว เหตุการณ์ด้านความปลอดภัยของข้อมูลประจำปียังคงอยู่ในระดับสูงคือ 166 เหตุการณ์ในปี 2023 และ 156 เหตุการณ์ในปี 2024 และความรุนแรงของเหตุการณ์เหล่านี้เพิ่มขึ้นจาก 20% ของเหตุการณ์ที่ถือว่ารุนแรง เป็น 27% ในปี 2024**

156

เหตุการณ์ด้านความปลอดภัยของข้อมูล

27%

ของเหตุการณ์ถือว่ารุนแรง
(เพิ่มขึ้นจาก 20% ในปี 2023)

63%

ของการแจ้งเตือนที่ได้รับการตรวจสอบต่อวัน

“ตำแหน่งที่แพลตฟอร์มซอฟต์แวร์ถูกสร้างขึ้นที่จัดเก็บข้อมูล และผู้ที่จะเข้าถึงข้อมูลดังกล่าวทำให้ความปลอดภัยของข้อมูลและการจัดการเครื่องมือ AI และผู้ขายของเรามีความซับซ้อน เรามีข้อมูลมากกว่า 100 ปีที่ต้องปกป้องและควบคุมตามข้อกำหนดทางกฎหมายในทุกเขตอำนาจศาลที่เราดำเนินงานอยู่” ผู้จัดการอาวุโสด้านการกำกับดูแลข้อมูลของผู้ผลิตเครื่องจักรกลหนักคนหนึ่งกล่าว

ความรุนแรงที่เพิ่มขึ้นของเหตุการณ์ด้านความปลอดภัยของข้อมูลนำไปสู่จำนวนการแจ้งเตือนที่เพิ่มขึ้น **องค์กรกำลังเผชิญการแจ้งเตือนเฉลี่ย 66 รายการต่อวัน เพิ่มขึ้นจาก 52 รายการในปี 2023** จำนวนดังกล่าวแตกต่างกันอย่างมากตามขนาดองค์กร โดยองค์กรขนาดกลาง (พนักงาน 500-999 คน) และองค์กรขนาดใหญ่ (พนักงาน 1,000-4,999 คน) ได้รับการแจ้งเตือนโดยเฉลี่ย 56 รายการ และองค์กรขนาดใหญ่พิเศษ (พนักงาน 5,000 คนขึ้นไป) ได้รับการแจ้งเตือนเฉลี่ย 80 รายการต่อวัน

เมื่อพิจารณาจากจำนวนการแจ้งเตือนด้านความปลอดภัยของข้อมูลที่สูงมากจึงไม่น่าแปลกใจที่องค์กรส่วนใหญ่ไม่สามารถรับมือได้ โดยเฉลี่ยแล้วทีมรักษาความปลอดภัยข้อมูลตรวจสอบการแจ้งเตือนรายวัน 63% 35% ของการแจ้งเตือนเหล่านี้พบว่าเป็นผลบวกลวง ความไม่ตรงกันระหว่างการควบคุมที่รับรู้และความเป็นจริงในการดำเนินงานนี้ทำให้ทีมรักษาความปลอดภัยข้อมูลหนักใจ — และพยายามประเมินว่าพวกเขามีการป้องกันที่เหมาะสมหรือไม่ หรือจะปรับแต่งการป้องกันเหล่านั้นอย่างไร พร้อมกันนี้ยังกังวลว่าเหตุการณ์ร้ายแรงที่เป็นไปได้อาจถูกมองข้ามไป

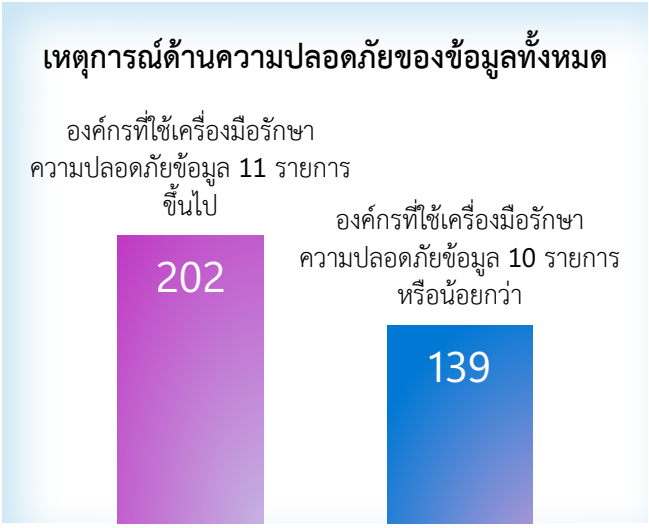
เพื่อต่อสู้กับความเสี่ยงของข้อมูลแบบดั้งเดิมและที่เกิดขึ้นใหม่ที่เชื่อมโยงกับการใช้เครื่องมือ AI กลยุทธ์การรักษาความปลอดภัยข้อมูลที่มีประสิทธิภาพและสอดคล้องกันมากขึ้นจึงมีความจำเป็นยิ่งขึ้น

แม้มีเครื่องมือจำนวนมากขึ้น แต่ผู้มีอำนาจตัดสินใจหลายคนยังคงยอมรับว่าจำนวนที่มากขึ้นไม่ได้ช่วยให้ดีขึ้นเสมอไป ในความเป็นจริง 21% ระบุว่าการขาดการมองเห็นที่ชัดเจนและครอบคลุม (และความเข้าใจร่วมกันเกี่ยวกับความเสี่ยง) ที่เกิดจากเครื่องมือที่แตกต่างกันเป็นความท้าทาย/ความเสี่ยงสำคัญที่สุด[1]

ผู้มีอำนาจตัดสินใจส่วนใหญ่ (82%) ยอมรับว่าแพลตฟอร์มแบบครบวงจรที่ครอบคลุมมีประสิทธิภาพมากกว่าการจัดการเครื่องมือที่แยกกันจำนวนมาก **โดยเฉลี่ยแล้วพวกเขากำลังพยายามจัดการโซลูชันการรักษาความปลอดภัยข้อมูลที่แตกต่างกัน 12 โซลูชัน ซึ่งสร้างความซับซ้อนที่ทำให้มีช่องโหว่มากขึ้น** สิ่งนี้เป็นจริงโดยเฉพาะอย่างยิ่งสำหรับองค์กรขนาดใหญ่ที่สุด: โดยเฉลี่ยแล้ว องค์กรขนาดกลางใช้เครื่องมือ 9 รายการ องค์กรขนาดใหญ่ใช้ 11 รายการ และองค์กรขนาดใหญ่พิเศษใช้ 14 รายการ

ข้อมูลแสดงความเชื่อมโยงที่แข็งแกร่งระหว่างจำนวนเครื่องมือรักษาความปลอดภัยข้อมูลที่ใช้กับความถี่ของเหตุการณ์ด้านความปลอดภัยของข้อมูล องค์กรขนาดกลางและขนาดใหญ่รายงานเหตุการณ์เฉลี่ย 89 เหตุการณ์ต่อปี ในขณะที่องค์กรขนาดใหญ่พิเศษเผชิญเหตุการณ์ถึง 248 เหตุการณ์ต่อปี ความแตกต่างอย่างชัดเจนนี้ชี้ให้เห็นว่าองค์กรขนาดใหญ่มีความเสี่ยงสูงแม้มีความเชื่อมั่นอย่างมากในมาตรการรักษาความปลอดภัยข้อมูลของตนเอง

ในปี 2024 องค์กรที่ใช้เครื่องมือรักษาความปลอดภัยข้อมูลมากกว่า (11 รายการขึ้นไป) ประสบเหตุการณ์ด้านความปลอดภัยของข้อมูลเฉลี่ย 202 เหตุการณ์ เทียบกับ139 เหตุการณ์สำหรับผู้ที่มีเครื่องมือ 10 รายการหรือน้อยกว่า



โซลูชันที่กระจัดกระจายทำให้ยากต่อการทำความเข้าใจมาตรการรักษาความปลอดภัยข้อมูล เนื่องจากข้อมูลถูกแยกจากกัน และเวิร์กโฟลว์ที่แตกต่างกันสามารถจำกัดการมองเห็นความเสี่ยงที่อาจเกิดขึ้นอย่างครอบคลุม เมื่อเครื่องมือไม่ผสานรวมกัน ทีมรักษาความปลอดภัยข้อมูลต้องสร้างกระบวนการเพื่อเชื่อมโยงข้อมูลและสร้างมุมมองความเสี่ยงที่สอดคล้องกันซึ่งอาจนำไปสู่จุดบอด และทำให้การตรวจหาและลดความเสี่ยงเหล่านั้นเป็นงานที่ท้าทาย

ความกังวลที่เพิ่มมากขึ้นคือการเพิ่มขึ้นของเหตุการณ์ด้านความปลอดภัยของข้อมูลจากการใช้แอปพลิเคชัน AI ซึ่งเพิ่มขึ้นเกือบสองเท่าจาก 27% ในปี 2023 เป็น 40% ในปี 2024 เหตุการณ์ที่เพิ่มขึ้นนี้เกิดจากการโจมตีของมัลแวร์และแรนซัมแวร์ที่เพิ่มขึ้นถึง 59% จาก 50% ในปี 2023 การโจมตีจากการใช้แอป AI ไม่เพียงเปิดเผยข้อมูลที่ละเอียดอ่อนเท่านั้น แต่ยังทำให้การทำงานของระบบ AI เสียหาย ส่งผลให้ภูมิทัศน์การรักษาความปลอดภัยข้อมูลที่กระจัดกระจายอยู่แล้วยิ่งซับซ้อนมากขึ้น กล่าวโดยสรุปคือ มีความจำเป็นเร่งด่วนมากขึ้นสำหรับกลยุทธ์การรักษาความปลอดภัยข้อมูลที่แข็งแกร่งและสอดคล้องกันมากขึ้น ซึ่งสามารถจัดการกับความเสี่ยงทั้งแบบดั้งเดิมและที่เกิดขึ้นใหม่ที่เชื่อมโยงกับการใช้เครื่องมือ AI

1. การสำรวจความคิดเห็นผู้รับผิดชอบความปลอดภัยของข้อมูลการกำกับดูแล และผู้มีอำนาจในการตัดสินใจประจำเดือนกันยายน 2024 ที่จัดทำโดย MDC Research ตามที่ได้รับมอบหมายจาก Microsoft

หนทางสู่อนาคต

ความรุนแรงที่เพิ่มขึ้นของเหตุการณ์ด้านความปลอดภัยของข้อมูลบ่งชี้โอกาสสำหรับ AI ในการให้ความช่วยเหลือ องค์กรล้ำสมัยกำลังปรับใช้การรักษาความปลอดภัยข้อมูลที่ขับเคลื่อนด้วย AI เพื่อช่วยจัดลำดับความสำคัญของเหตุการณ์ จัดประเภทข้อมูลโดยอัตโนมัติ และระบุวิธีการปรับแต่งนโยบายการป้องกันปัจจุบัน AI สามารถสังเคราะห์การแจ้งเตือนความรุนแรงที่อาจเกิดขึ้นของเหตุการณ์โดยอัตโนมัติ ทำให้ทีมรักษาความปลอดภัยข้อมูลมีข้อมูลเชิงลึกที่นำไปปฏิบัติได้เพื่อการตอบสนองอย่างรวดเร็วซึ่งจะลดเวลาที่ต้องใช้กับผลบวกลวง วิธีนี้ช่วยปรับปรุงเวิร์กโฟลว์และช่วยให้ทีมรักษาความปลอดภัยข้อมูลสามารถมุ่งเน้นการปรับปรุงการรักษาความปลอดภัยข้อมูลเชิงกลยุทธ์และมาตรการเชิงรุกมากขึ้น

2

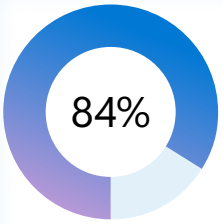
การที่ผู้ใช้นำแอป AI มาใช้มากขึ้น ส่งผลให้ความสมบูรณ์ของข้อมูลที่ละเอียดอ่อนที่สุดขององค์กรมีความเสี่ยงมากขึ้น ซึ่งต้องการการมองเห็นและการควบคุมการป้องกันใหม่ๆ มากขึ้น

AI กลายเป็นสิ่งจำเป็นสำหรับการทำงานประจำวันอย่างรวดเร็ว และองค์กรต้องเปิดรับและปรับตัวให้เข้ากับความเป็นจริงใหม่ดังกล่าวอย่างจริงจัง

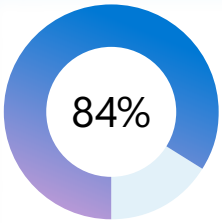
การนำเครื่องมือ AI มาใช้อย่างรวดเร็วของพนักงานได้กระตุ้นให้เกิดการเปลี่ยนแปลงครั้งใหญ่ในแนวทางเพื่อความปลอดภัยของข้อมูลขององค์กร ขณะที่ AI กำลังเปลี่ยนแปลงประสิทธิภาพการทำงานและเวิร์กโฟลว์ เช่นเดียวกับเทคโนโลยีที่เกิดขึ้นใหม่ AI ยังอาจทำให้ความเสี่ยงที่มีอยู่เดิมเพิ่มขึ้น หรือนำมาซึ่งความเสี่ยงใหม่ๆ ที่ต้องใช้วิธีการที่แตกต่างกันในการปกป้องข้อมูลที่ละเอียดอ่อน ด้วยเหตุนี้ บริษัทต่างๆ จึงเริ่มทำความคุ้นเคยกับภูมิทัศน์ที่เปลี่ยนแปลงอย่างรวดเร็ว ผู้อำนวยการฝ่ายวิศวกรรมและการวิเคราะห์ด้านการขนส่งคนหนึ่งกล่าวว่า "เรากำลังตรวจสอบข้อมูลด้าน AI อย่างรอบคอบมากขึ้น มีความตึงเครียดระหว่างการผลิตและการรักษาความปลอดภัย ความแม่นยำ และความเป็นส่วนตัว"

ความเชื่อมั่นในการรักษาความปลอดภัยในการใช้ AI ของพนักงานยังคงมีความแตกต่างหลากหลาย โดยส่วนใหญ่ (84%) ต้องการรู้สึกมั่นใจมากขึ้นเกี่ยวกับการจัดการและการค้นพบการป้อนข้อมูล ขณะที่ 22% ขององค์กรรู้สึกมั่นใจอย่างยิ่งในความสามารถในการรักษาความปลอดภัยข้อมูลของตนเอง และส่วนใหญ่ (59%) แค่ “มั่นใจมาก” ซึ่งบ่งชี้ว่ายังมีส่วนที่ต้องการการปรับปรุง บริษัทส่วนใหญ่ (86%) ยอมรับว่าพวกเขาต้องการรู้สึกมั่นใจมากขึ้นเกี่ยวกับการจัดการและการค้นพบข้อมูลที่สร้างขึ้นโดยเครื่องมือ AI

ขณะที่ AI กลายเป็นสิ่งจำเป็นมากขึ้นสำหรับการทำงานในแต่ละวัน การใช้แอป AI ยังเพิ่มความกังวลเกี่ยวกับเหตุการณ์ด้านความปลอดภัยของข้อมูลอีกด้วย **เกือบหนึ่งในสาม (31%) ขององค์กรคาดการณ์ว่าเหตุการณ์ด้านความปลอดภัยของข้อมูลจะเพิ่มขึ้นเนื่องจากการใช้ AI ของพนักงาน และ 84% ยอมรับว่าจำเป็นต้องพยายามมากขึ้นเพื่อป้องกันความเสี่ยงเหล่านี้** ความกังวลดังกล่าวยิ่งสูงขึ้นโดยเฉพาะอย่างยิ่งในองค์กรขนาดใหญ่ที่สุด: ขณะที่มีองค์กรขนาดกลางเพียง 26% คาดว่าจะเห็นการเพิ่มขึ้นของเหตุการณ์ด้านความปลอดภัยของข้อมูลที่เกี่ยวข้องกับ AI และ 29% สำหรับองค์กรขนาดใหญ่ แต่สำหรับองค์กรขนาดใหญ่พิเศษที่คาดการณ์แบบเดียวกันนี้มีจำนวนสูงถึง 36%



ต้องการรู้สึกมั่นใจมากขึ้นเกี่ยวกับการจัดการและการค้นพบการป้อนข้อมูลลงในแอปและเครื่องมือ AI



ยอมรับว่าจำเป็นต้องพยายามมากขึ้นเพื่อป้องกันการใช้แอปและเครื่องมือ AI ของพนักงานที่มีความเสี่ยง

มีการใช้ AI ที่ไม่ได้รับอนุญาตอย่างแพร่หลาย

40% รายงานว่าแอป AI ของพวกเขาถูกละเมิดหรือถูกบุกรุกในเหตุการณ์ความปลอดภัยของข้อมูล เช่นเดียวกัน ตัวเลขนี้สูงขึ้นในหมู่องค์กรขนาดใหญ่: องค์กรขนาดกลางรายงานเหตุการณ์ดังกล่าวในอัตรา 36%, องค์กรขนาดใหญ่รายงาน 38% และองค์กรขนาดใหญ่พิเศษเผชิญเหตุการณ์ดังกล่าวมากที่สุดคือ 44%

การใช้ AI ที่ไม่ได้รับอนุญาตมักเกิดขึ้นกับพนักงานที่เข้าสู่ระบบด้วยข้อมูลประจำตัวส่วนบุคคล หรือใช้อุปกรณ์ส่วนบุคคลสำหรับภารกิจที่เกี่ยวข้องกับงาน **โดยเฉลี่ยแล้วองค์กร 65% ยอมรับว่าพนักงานของตนใช้เครื่องมือ AI ที่ไม่ได้รับอนุญาต** พนักงานใช้เครื่องมือ AI ที่ไม่ได้รับอนุญาตในรูปแบบดังต่อไปนี้:

- 53% เข้าสู่ระบบด้วยข้อมูลประจำตัวส่วนบุคคลเพื่อวัตถุประสงค์ในการทำงาน
- 48% ใช้อุปกรณ์ส่วนตัวเมื่อใช้ AI ในการทำงาน
- 47% ใช้ข้อมูลประจำตัวในการทำงานเพื่อใช้ AI สำหรับวัตถุประสงค์ส่วนตัว

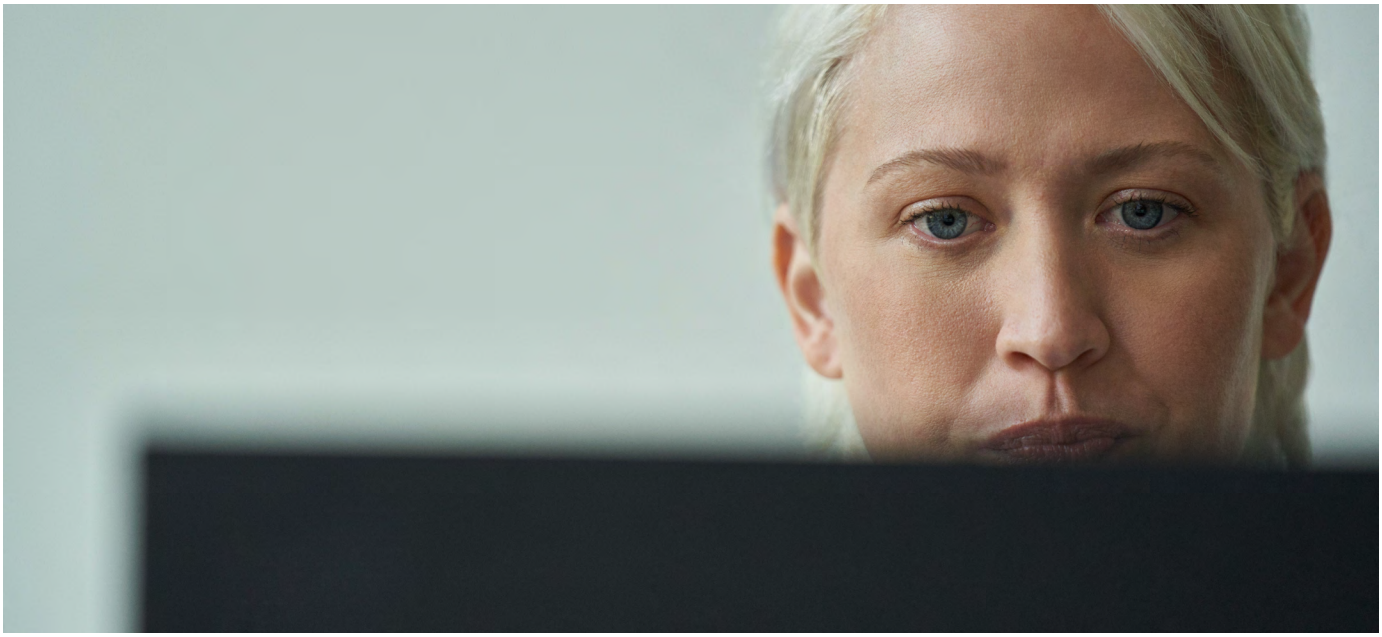
ครึ่งหนึ่งขององค์กรทั้งหมดระบุว่าพวกเขากังวลเกี่ยวกับการขาดการควบคุมเพื่อตรวจหาและลดความเสี่ยงเมื่อพนักงานใช้แอป AI ในวิธีที่ไม่ปลอดภัย ตัวเลขนี้แตกต่างกันไปตามขนาดบริษัท โดย 43% ขององค์กรขนาดกลาง, 50% ขององค์กรขนาดใหญ่ และ 54% ขององค์กรขนาดใหญ่พิเศษแสดงความกังวลเกี่ยวกับความสามารถในการจัดการความเสี่ยงเหล่านี้

เมื่อพิจารณาจากการใช้ AI ที่เพิ่มขึ้น จึงจำเป็นต้องมีการควบคุมความปลอดภัยของข้อมูลมากขึ้น

ขณะที่ AI ฝังตัวในการดำเนินงานประจำวันมากขึ้น องค์กรจึงตระหนักถึงความจำเป็นในการป้องกันที่แข็งแกร่งขึ้น **แม้บริษัท 96% กังวลเกี่ยวกับการใช้เครื่องมือเหล่านี้ของพนักงาน แต่ส่วนใหญ่ยินดีลงทุนในโซลูชันต่างๆ เพื่อเอาชนะความกังวลเหล่านั้น**

“โฟกัสสำคัญจะอยู่ที่ทำอย่างไรจึงจะก้าวล้ำนำหน้า AI ได้ การมุ่งเน้นด้านความปลอดภัยเป็นเรื่องเกี่ยวกับการลดขนาดข้อมูล การตรวจสอบข้อมูลอย่างระมัดระวังมากขึ้น ในด้าน AI นั้น เพื่อให้โมเดลของคุณเป็นตัวอย่างในการระบุความโน้มเอียงมากขึ้น คุณจำเป็นต้องมีข้อมูลเพิ่มเติม ถ้าเช่นนั้นคุณจะประนีประนอมอย่างไร” ผู้อำนวยการฝ่ายวิศวกรรมสถาปัตยกรรม และการวิเคราะห์ในการขนส่งกล่าว ผู้มีอำนาจตัดสินใจส่วนใหญ่ (87%) พร้อมที่จะใช้เวลาและเงินกับการฝึกอบรมพนักงานในการปฏิบัติที่ปลอดภัยสำหรับการใช้เครื่องมือ AI **โดย 85% ระบุว่าพนักงานจำเป็นต้องใช้เครื่องมือเหล่านี้ในการแข่งขัน**

เกือบทุกองค์กร (93%) อยู่ในขั้นตอนการพัฒนาหรือดำเนินการควบคุมเกี่ยวกับการใช้ AI แต่หลายองค์กรยังคงอยู่ในช่วงเริ่มต้นเท่านั้น มีเพียง 39% ที่สามารถใช้การควบคุมความปลอดภัยของข้อมูลสำหรับ AI อย่างเต็มที่ ขณะที่ 24% ได้พัฒนานโยบายแต่ยังไม่ได้นำมาใช้จริง รองประธานฝ่ายความปลอดภัยของข้อมูลในธุรกิจบริการต้อนรับผู้หนึ่งกล่าวว่า “เราต้องปรับแนวทางการควบคุมให้สอดคล้องกับสำหรับ AI ขณะที่เราเปิดรับการใช้ AI ไปพร้อมกัน ซึ่งทำให้ชีวิตดีขึ้นและช่วยให้เราทำงานอย่างมีประสิทธิภาพมากขึ้น”



ขณะที่องค์กรกำลังดำเนินการเพื่อปกป้องข้อมูลที่ละเอียดอ่อนจากการนำไปใช้ในทางที่ผิดในแอป AI มีความจำเป็นอย่างชัดเจนสำหรับการควบคุมที่ครอบคลุมมากขึ้น ปัจจุบัน บริษัท 43% มุ่งเน้นการป้องกันข้อมูลที่ละเอียดอ่อนจากการอัปโหลดไปยังแอป AI ขณะที่อีก 42% กำลังบันทึกกิจกรรมและเนื้อหาทั้งหมดภายในแอปเหล่านี้เพื่อการตรวจสอบหรือการตอบสนองเหตุการณ์ที่อาจเกิดขึ้น เช่นเดียวกัน บริษัท 42% กำลังปิดกั้นการเข้าถึงเครื่องมือที่ไม่ได้รับอนุญาตของผู้ใช้ และบริษัทจำนวนพอๆ กันนี้กำลังลงทุนในการฝึกอบรมพนักงานเกี่ยวกับการใช้ AI อย่างปลอดภัย

บริษัทที่มีพนักงานที่มีส่วนร่วมในการใช้งาน AI ที่ไม่ได้รับอนุญาตมีความต้องการการควบคุมบางประเภทมากขึ้น **ในบรรดาบริษัทที่มีการใช้งาน AI โดยไม่ได้รับอนุญาต 42% ต้องการการควบคุมเพื่อระบุผู้ใช้ที่มีความเสี่ยงโดยอิงกับการสอบถามของ AI เทียบกับ 30% สำหรับบริษัทที่ไม่มีการใช้ AI โดยไม่ได้รับอนุญาต นอกจากนี้ 40% ขององค์กรที่จัดการการใช้ AI ที่ไม่ได้รับอนุญาตต้องการการควบคุมเพื่อจัดการวงจรชีวิตของข้อมูล (เช่น โปรโตคอลการเก็บข้อมูลและการลบ) เทียบกับ 27% ของบริษัทที่ไม่มีปัญหานี้**

การควบคุม AI 5 อันดับแรกที่จำเป็น

ป้องกันข้อมูลที่ละเอียดอ่อนจากการอัปโหลดไปยัง AI	43%
บันทึกกิจกรรมและเนื้อหาทั้งหมดในเครื่องมือ AI เพื่อการตรวจสอบหรือการตอบสนองเหตุการณ์ที่อาจเกิดขึ้น	42%
ปิดกั้นการเข้าถึงเครื่องมือ AI ที่ไม่ได้รับอนุญาตของผู้ใช้	42%
ฝึกอบรมพนักงานเกี่ยวกับการใช้เครื่องมือ AI อย่างปลอดภัย	42%
ระบุผู้ใช้ที่มีความเสี่ยงโดยอิงจากการสอบถามใน AI	41%

หนทางสู่อนาคต

เพื่อดำเนินมาตรการรักษาความปลอดภัยข้อมูลที่แข็งแกร่ง ทีมจำเป็นต้องมีชุดการควบคุมที่สมบูรณ์เพื่อค้นหา ปกป้อง และควบคุมข้อมูลของตนในแอป AI ต่อไปนี้คือกลยุทธ์สำคัญสามประการที่ทีมสามารถใช้ได้:

เพิ่มความสามารถในการมองเห็นการใช้แอป AI และข้อมูลที่ไหลผ่านแอป: ใช้เครื่องมือรักษาความปลอดภัยข้อมูลที่สามารถตรวจหาและใช้งานแอป AI ได้ เครื่องมือเหล่านี้ให้ข้อมูลเชิงลึกเกี่ยวกับรายการแอป AI ที่ครอบคลุมที่ใช้ร่วมกับโปรไฟล์ความเสี่ยง รวมถึงรายละเอียด เช่น การควบคุมความปลอดภัยของข้อมูลที่ได้รับการสนับสนุน และการปฏิบัติตามข้อบังคับ ใช้เครื่องมือที่สามารถจัดประเภทที่สอดคล้องกันสำหรับข้อมูลที่ละเอียดอ่อนในการโต้ตอบกับ AI และแสดงแนวโน้มเกี่ยวกับวิธีการที่ข้อมูลไหลผ่านแอป AI

พัฒนาและบังคับใช้นโยบาย: สร้างนโยบายตามข้อมูลเชิงลึกที่ได้รับจากการวิเคราะห์ นโยบายเหล่านี้อาจรวมถึงแนวทางสำหรับแอป AI ที่ได้รับการอนุมัติ และขั้นตอนในการปิดกั้นหรือจำกัดการใช้แอปที่ไม่ได้รับอนุมัติของพนักงาน แม้ในแอป AI ที่ได้รับอนุมัติ คุณสามารถสร้างนโยบายอย่างละเอียดเพื่อให้ข้อมูลที่ไม่ใช่ข้อมูลละเอียดอ่อนไหลผ่านได้ควบคู่กับการจำกัดการใช้ข้อมูลที่ละเอียดอ่อนและข้อมูลสำคัญทางธุรกิจ ซึ่งอาจรวมถึงการปิดกั้นการกระทำบางอย่าง เช่น การวางข้อมูลที่ละเอียดอ่อนลงในเครื่องมือ AI บนเบราว์เซอร์เพื่อให้แน่ใจว่าข้อมูลมีความปลอดภัย

ประเมินความเสี่ยงและปรับแต่งนโยบายเป็นประจำ: สร้างรายงานที่แสดงระดับความเสี่ยงของแอป AI ที่ใช้อยู่เป็นประจำ แนวโน้มเกี่ยวกับวิธีที่ข้อมูลที่ละเอียดอ่อนไหลผ่านแอปเหล่านี้ รวมถึงกิจกรรมของผู้ใช้ในแอปเหล่านี้ วิธีนี้ช่วยในการประเมินภูมิทัศน์ความเสี่ยงโดยรวมและการตัดสินใจโดยใช้ข้อมูลประกอบเกี่ยวกับนโยบายความปลอดภัยของข้อมูลที่เกี่ยวข้องมากที่สุด

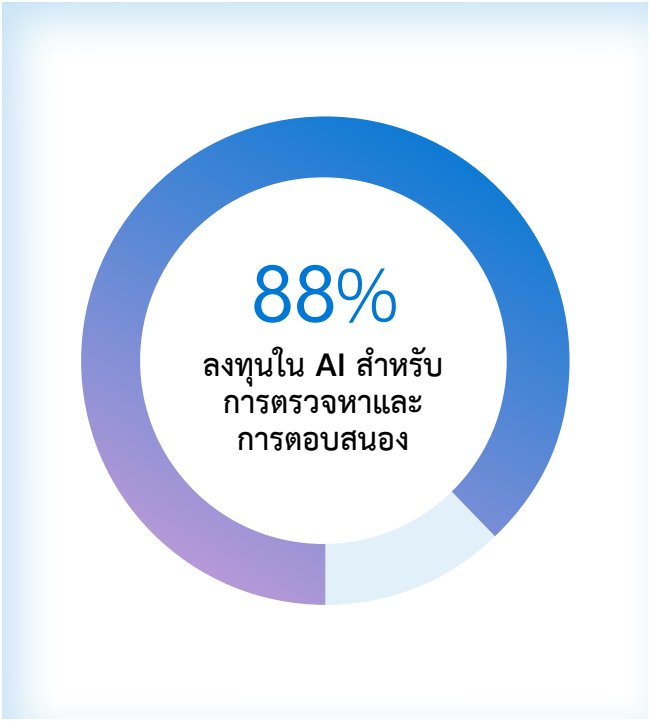
3

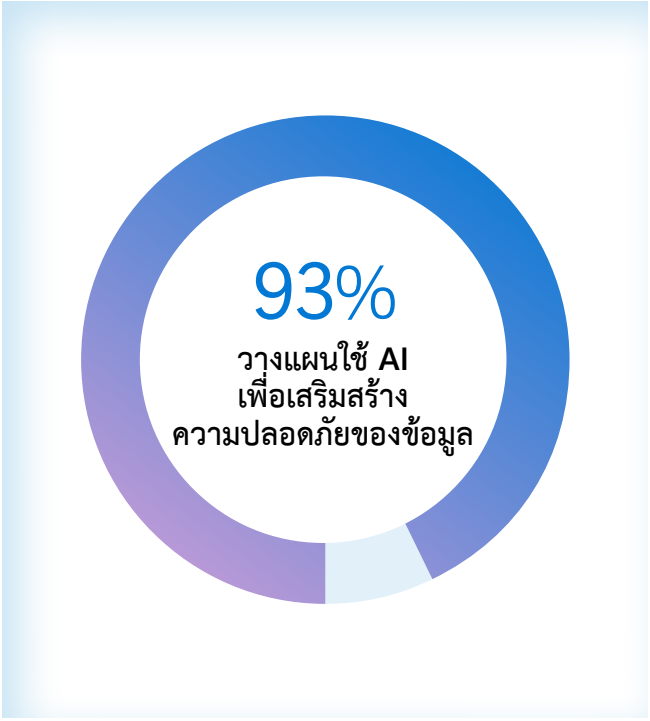
ผู้มีอำนาจตัดสินใจมองโลกในแง่ดีเกี่ยวกับศักยภาพของ AI ในการเพิ่มความพยายามด้านความปลอดภัยของข้อมูล

การตรวจสอบความปลอดภัยของข้อมูลต้องพึ่งพา AI อย่างมาก

องค์กรส่วนใหญ่ (88%) กำลังลงทุนใน AI เพื่อปรับปรุงความพยายามในการตรวจหาและการตอบสนอง ซึ่งหมายถึงการค้นพบข้อมูลที่ละเอียดอ่อน การตรวจหากิจกรรมที่ผิดปกติ และการป้องกันข้อมูลที่มีความเสี่ยงโดยอัตโนมัติ **องค์กร 77% เชื่อว่า AI จะเร่งกระบวนการเหล่านี้ และ 76% คิดว่า AI จะปรับปรุงความเที่ยงตรงของกลยุทธ์การตรวจจับและการตอบสนองขององค์กร**

ขณะที่ผู้มีอำนาจตัดสินใจ 73% แสดงความกังวลเกี่ยวกับการใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูล, 50% ระบุว่าไม่ได้ห้ามการใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูล และมีเพียง 23% เท่านั้นที่ห้ามใช้ ผู้มีอำนาจตัดสินใจจำนวนถึง 93% อย่างน้อยที่สุดกำลังวางแผนใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูลแม้มีข้อกังวลก็ตาม

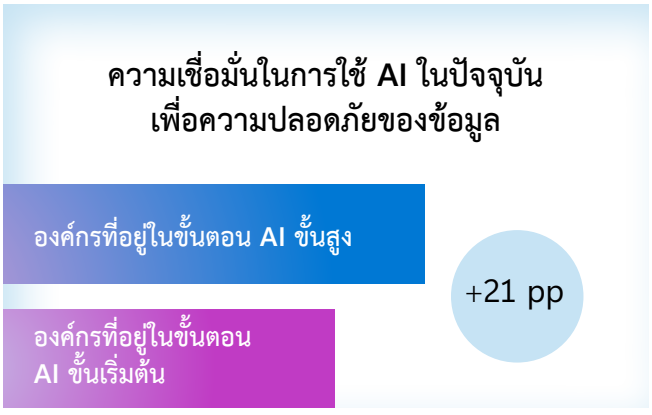


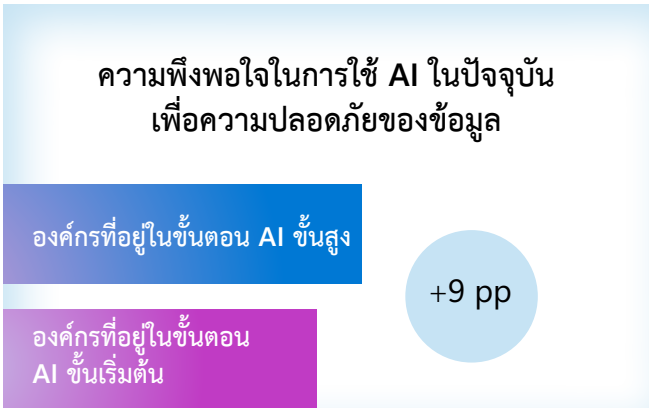


การใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูลช่วยเพิ่มการมองเห็น ความเชื่อมั่น และความพึงพอใจ

หนึ่งในประโยชน์ที่สำคัญของการใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูลคือความสามารถในการเพิ่มการมองเห็นทั่วทั้งระบบ ซึ่งช่วยลดความกังวลสำคัญของผู้มีอำนาจตัดสินใจที่ต้องการรู้ว่าข้อมูลถูกเก็บไว้ที่ใดและได้รับการจัดประเภทอย่างไร (20%)[1] 88% ของผู้มีอำนาจตัดสินใจด้านความปลอดภัยของข้อมูลเชื่อว่าการผนวกรวม AI เข้ากับโซลูชันความปลอดภัยของข้อมูลจะช่วยให้ทีมมองเห็นได้ชัดเจนขึ้น ซึ่งจะช่วยให้องค์กรสามารถประมวลผลและวิเคราะห์ข้อมูลเพิ่มขึ้นอย่างมาก องค์กรขนาดกลางมุ่งเน้นการลดความเสี่ยงระยะสั้นเป็นหลัก เช่น การลดข้อผิดพลาดของมนุษย์ในกระบวนการรักษาความปลอดภัยข้อมูล ในความเป็นจริง องค์กรขนาดกลาง 43% ให้ความสำคัญกับการลดความเสี่ยงที่เกิดจากความผิดพลาดของมนุษย์ เทียบกับเพียง 37% ขององค์กรขนาดใหญ่พิเศษ ในทางกลับกัน องค์กรขนาดใหญ่มีความก้าวหน้ามากขึ้นในแนวทางของตนเอง โดยเน้นความเสี่ยงระยะยาวและความต้องการในการปรับตัวความซับซ้อนในระดับที่สูงขึ้นดังกล่าวช่วยให้ทีมรักษาความปลอดภัยข้อมูลสามารถปรับตัวให้เข้ากับความเสี่ยงที่เปลี่ยนแปลงตลอดเวลาได้ดีขึ้น ซึ่งเป็นเป้าหมายสำคัญสูงสุดสำหรับองค์กรขนาดใหญ่พิเศษ 49% เทียบกับ 43% ขององค์กรขนาดกลาง

โดยรวมแล้ว องค์กรที่นำหน้าในการใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูลรายงานความมั่นใจและความพึงพอใจในกลยุทธ์การรักษาความปลอดภัยของข้อมูลในระดับที่สูงขึ้นมาก **ในบรรดาองค์กรที่อยู่ในขั้นตอนการใช้งาน AI ขั้นสูงนั้น 90% รู้สึกมั่นใจมากหรือมั่นใจอย่างยิ่งในการใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูล เทียบกับ 69% ขององค์กรที่อยู่ในขั้นตอนต้นๆ ของการปรับใช้ AI ในทำนองเดียวกัน 76% ขององค์กรที่มีการใช้งาน AI ขั้นสูงแสดงความพึงพอใจกับโซลูชันความปลอดภัยของข้อมูล ขณะที่องค์กรที่อยู่ในขั้นตอนต้นๆ ของการปรับใช้ AI เพียง 67% ที่รายงานแบบเดียวกัน**





1. การสำรวจความคิดเห็นผู้รับผิดชอบความปลอดภัยของข้อมูล การกำกับดูแล การปฏิบัติตามข้อบังคับ และ ผู้มีอำนาจตัดสินใจด้านความเป็นส่วนตัวที่จัดทำโดย MDC Research ตามที่ได้รับมอบหมายจาก Microsoft

องค์กรต่างๆ กำลังลดจำนวนเหตุการณ์ด้านความปลอดภัยของข้อมูล และปรับปรุงการจัดการการแจ้งเตือนด้วย AI

องค์กรที่ใช้ AI เพื่อเสริมสร้างการดำเนินงานด้านความปลอดภัยของข้อมูลรายงานการแจ้งเตือนน้อยลงอย่างมาก **โดยเฉลี่ยแล้ว องค์กรที่ใช้เครื่องมือรักษาความปลอดภัยข้อมูลที่ขับเคลื่อนด้วย AI จะได้รับการแจ้งเตือน 47 รายการต่อวัน เทียบกับการแจ้งเตือน 79 รายการสำหรับองค์กรที่ไม่มีเครื่องมือดังกล่าว และองค์กรที่ใช้ AI สามารถตรวจสอบการแจ้งเตือนรายวันได้ 66% ขณะที่องค์กรที่ไม่ได้ใช้ AI จัดการการตรวจสอบได้เพียง 60%**

นอกจากนี้ องค์กรที่ใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูลยังมีแนวโน้มใช้ AI เพื่อลดความเสี่ยง (56% เทียบกับ 26%) จำนวนการแจ้งเตือนที่ลดลง ตลอดจนถึงความสามารถในการลดการแจ้งเตือนโดยใช้ประโยชน์จาก AI ที่เพิ่มขึ้น ดูเหมือนมีผลกระทบอย่างมากต่อจำนวนเหตุการณ์ด้านความปลอดภัยของข้อมูลโดยรวม องค์กรที่นำ AI มาใช้เพื่อเสริมสร้างความปลอดภัยของข้อมูลรับรู้ว่าเหตุการณ์ด้านความปลอดภัยของข้อมูลลดลง 65% เทียบกับองค์กรที่ไม่ได้ใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูล

AI ถูกคาดว่าจะมีผลกระทบต่อการตอบสนองมากที่สุด

ในแง่การตรวจหา ผู้มีอำนาจตัดสินใจ 33% คาดว่า AI จะช่วยตรวจหากิจกรรมผิดปกติ ขณะที่ 23% เชื่อว่าจะช่วยในการตรวจสอบเหตุการณ์ด้านความปลอดภัยของข้อมูลที่อาจเกิดขึ้น อีก 22% เห็นศักยภาพของ AI ในการให้คำแนะนำเพื่อรักษาความปลอดภัยสภาพแวดล้อมของข้อมูลอย่างดียิ่งขึ้น

อย่างไรก็ตาม การตอบสนองคือสิ่งที่ผู้มีอำนาจตัดสินใจคาดหวังว่า AI จะสร้างผลกระทบที่ลึกซึ้งที่สุด ผู้มีอำนาจตัดสิน 34% เชื่อว่า AI สามารถปิดกั้นการแบ่งปันข้อมูลที่ละเอียดอ่อนที่ไม่เหมาะสมโดยอัตโนมัติ และ 32% ระบุว่า AI จะปกป้องข้อมูลที่มีความเสี่ยง อีก 26% รับรู้ว่า AI ช่วยลดความเสี่ยงด้านความปลอดภัยของข้อมูลและใช้การควบคุมที่เหมาะสม ขณะที่ผู้มีอำนาจตัดสินใจจำนวนเท่ากันคาดว่า AI จะตั้งค่าสถานะพฤติกรรมของผู้ใช้ที่มีความเสี่ยงโดยอัตโนมัติ

หนทางสู่อนาคต

การผสานรวม AI เข้ากับโซลูชันการรักษาความปลอดภัยข้อมูลสามารถช่วยได้โดยการนำเสนอคำแนะนำในเวลาจริง ความสามารถในการสรุป และการสนับสนุนภาษาธรรมชาติไปยังส่วนที่เป็นที่สนใจแต่อาจถูกมองข้ามไป วิธีนี้ยังสามารถเร่งการตรวจสอบและส่งเสริมความเชี่ยวชาญของทีมรักษาความปลอดภัยข้อมูล ต่อไปนี้คือวิธีที่ความสามารถเหล่านี้สามารถสร้างผลกระทบ:

การสรุปการแจ้งเตือน: การตรวจสอบอาจเป็นงานที่ท้าทายเนื่องจากจำนวนแหล่งที่มาในการวิเคราะห์และกฎนโยบายที่หลากหลาย การฝัง AI ในการป้องกันการสูญหายของข้อมูล (DLP) และการจัดการความเสี่ยงภายใน (IRM) ทำให้ทีมได้รับข้อมูลสรุปการแจ้งเตือนได้อย่างรวดเร็ว รวมถึงแหล่งที่มา กฎนโยบาย และข้อมูลเชิงลึกเกี่ยวกับความเสี่ยงของผู้ใช้เพื่อทำความเข้าใจว่าข้อมูลที่ละเอียดอ่อนใดที่ถูกบุกรุกและความเสี่ยงของผู้ใช้ที่เกี่ยวข้อง

การสื่อสารที่อิงกับบริบท: องค์กรต้องปฏิบัติตามข้อกำหนดด้านกฎระเบียบเกี่ยวกับการสื่อสารทางธุรกิจ ซึ่งมักจำเป็นต้องตรวจสอบการละเมิดอย่างครอบคลุม AI สามารถช่วยทีมรักษาความปลอดภัยข้อมูลในการประเมินเนื้อหาที่ละเมิดกฎระเบียบและนโยบายขององค์กร เพื่อระบุการสื่อสารที่มีความเสี่ยงสูงที่อาจส่งผลให้เกิดเหตุการณ์ด้านความปลอดภัยของข้อมูล

ภาษาธรรมชาติในการสอบถามคำสำคัญ: การค้นหาอาจเป็นเวิร์กโฟลว์ที่ซับซ้อนและใช้เวลานานในระหว่างการตรวจสอบ ซึ่งโดยทั่วไปต้องใช้ภาษาการสอบถามด้วยคำหลัก AI ช่วยให้ทีมรักษาความปลอดภัยข้อมูลป้อนพร้อมท์การค้นหาด้วยภาษาธรรมชาติเพื่อปรับปรุงการเริ่มต้นการค้นหาและเปิดใช้งานการตรวจสอบขั้นสูงมากขึ้น

คำแนะนำสุดท้าย

1 ป้องกันความเสี่ยงจากเหตุการณ์ด้านความปลอดภัยของข้อมูลโดยการนำแพลตฟอร์มแบบผสานรวมมาใช้

การปรับใช้แพลตฟอร์มการรักษาความปลอดภัยข้อมูลแบบครบวงจรนำเสนอกลยุทธ์ที่ปลอดภัยและมีประสิทธิภาพมากขึ้นในภูมิทัศน์ที่มีการเปลี่ยนแปลงมากขึ้น ลดความซับซ้อนและเพิ่มการมองเห็นควบคู่กับการปรับปรุงการป้องกัน แนวทางแบบผสานรวมสามารถช่วยองค์กรในการปรับปรุงการจัดการมาตรการรักษาความปลอดภัยข้อมูล โดยการรวมศูนย์การควบคุมความปลอดภัยของข้อมูล และให้การมองเห็นครบวงจรสำหรับข้อมูล ผู้ใช้ และกิจกรรมทั้งหมด จึงเสริมสร้างและปรับปรุงการตรวจหาและการป้องกันความเสี่ยงของข้อมูล การที่องค์กร 82% ยอมรับว่าแพลตฟอร์มแบบผสานรวมเหนือชั้นกว่า การย้ายไปสู่การผสานรวมจึงไม่ได้เป็นประโยชน์เท่านั้น — แต่ยังเป็นสิ่งสำคัญ

2 เพิ่มความสามารถในการมองเห็นการใช้ AI ภายในในการ ประเมินการควบคุมที่จำเป็นสำหรับการใช้ AI ของพนักงานของ AI ที่จะไม่ส่งผลกระทบต่อประสิทธิภาพการทำงาน

การที่ AI กลายเป็นสิ่งที่พบได้ทั่วไปในที่ทำงานมากขึ้น AI จึงสามารถเพิ่มความเสี่ยงที่มีอยู่เดิมและนำไปสู่ความเสี่ยงใหม่ๆ ได้ องค์กรต่างๆ ยอมรับว่าจำเป็นต้องพยายามมากขึ้นเพื่อป้องกันการใช้ AI ที่ไม่ปลอดภัย การใช้การควบคุมในตัวและความสามารถในการมองเห็นในแอป AI เป็นสิ่งสำคัญในการรักษาความปลอดภัยข้อมูลโดยไม่ส่งผลกระทบต่อประสิทธิภาพการทำงาน การฝึกอบรมพนักงานเกี่ยวกับการใช้ AI อย่างปลอดภัยสามารถช่วยให้องค์กรลดพฤติกรรมเสี่ยง โดยมั่นใจได้ว่าทีมจะยังคงได้รับประโยชน์จากเครื่องมือที่มีประสิทธิภาพเหล่านี้ต่อไป

3 ยกระดับกลยุทธ์การรักษาความปลอดภัยข้อมูลของคุณด้วยความช่วยเหลือจาก AI

AI ช่วยให้ทีมรักษาความปลอดภัยข้อมูลสามารถมุ่งเน้นที่แนวคิดริเริ่มเชิงกลยุทธ์มากขึ้น แทนที่จะตอบสนองต่อภัยคุกคามที่เกิดขึ้นอย่างต่อเนื่องและการแจ้งเตือนจำนวนมาก บริษัทที่อยู่ในขั้นตอนการปรับใช้ AI ขั้นสูงมีความมั่นใจและพึงพอใจมากขึ้นกับโซลูชันการรักษาความปลอดภัยข้อมูลมากกว่าบริษัทที่เพิ่งเริ่มต้น โดยการปรับใช้ AI เป็นส่วนหนึ่งของกลยุทธ์การรักษาความปลอดภัยข้อมูลที่ครอบคลุม องค์กรสามารถเพิ่มการมองเห็น ซึ่งเสริมสร้างความสามารถในการตรวจหาและการตอบสนองต่อความเสี่ยงและส่งเสริมมาตรการรักษาความปลอดภัยของข้อมูลโดยรวมในท้ายที่สุด

วัตถุประสงค์ของการวิจัย

วัตถุประสงค์ของการวิจัยประกอบด้วย:

1. ทำความเข้าใจภูมิทัศน์ความปลอดภัยของข้อมูล รวมถึงลำดับความสำคัญและแนวคิดความท้าทาย ตลอดจนสาเหตุ และผลกระทบของเหตุการณ์ด้านความปลอดภัยของข้อมูล
2. สำรวจอนาคตของความปลอดภัยของข้อมูล รวมถึงกลยุทธ์และนวัตกรรมที่เกิดขึ้นใหม่ และสำรวจว่าองค์กรตั้งใจจะลงทุนในอนาคตอย่างไร
3. ค้นพบบทบาทของ AI ในการเพิ่มประสิทธิภาพความปลอดภัยของข้อมูลและบทบาทของ AI ในการปกป้องข้อมูล

วิธีการ

แบบสำรวจความคิดเห็นออนไลน์ในหลายประเทศ ความยาว 20 นาที จัดทำขึ้นระหว่างวันที่ 5-23 สิงหาคม 2024 ในกลุ่มผู้มีอำนาจตัดสินใจด้านความปลอดภัยของข้อมูล 1,376 ราย

คำถามมุ่งเน้นเกี่ยวกับภูมิทัศน์ด้านความปลอดภัยของข้อมูลและเหตุการณ์ด้านความปลอดภัยของข้อมูลเปรียบเทียบกับปี 2023 นอกจากนี้ การสำรวจในปีนี้ยังรวมถึงคำถามเกี่ยวกับการรักษาความปลอดภัยให้กับพนักงานในการใช้ AI และการใช้ AI เพื่อเสริมสร้างความปลอดภัยของข้อมูล

การสรรหากลุ่มเป้าหมาย

เพื่อให้เป็นไปตามเกณฑ์การคัดกรอง ผู้มีอำนาจตัดสินใจด้านความปลอดภัยของข้อมูลต้องเป็น:

- CISO และผู้มีอำนาจตัดสินใจที่อยู่ระดับใกล้เคียงกัน (C-2 ขึ้นไป) ที่มีหน้าที่รับผิดชอบความปลอดภัยของข้อมูล
- ทำงานในองค์กร (พนักงาน 500 คนขึ้นไป; หลากหลายขนาด)
- การผสมผสานระหว่างอุตสาหกรรมที่ได้รับการควบคุมและไม่ได้รับการควบคุม (ไม่ใช่อุตสาหกรรมด้านการศึกษา รัฐบาล หรือองค์กรไม่แสวงหาผลกำไร)

จากผู้มีอำนาจตัดสินใจด้านความปลอดภัยของข้อมูล 1,376 รายที่ได้รับการสำรวจสำหรับการวิจัยนี้ซึ่งแบ่งตามประเทศ ได้แก่:

- สหรัฐอเมริกา: 302 ราย
- สหราชอาณาจักร: 305 ราย
- อินเดีย: 301 ราย
- บราซิล: 158 ราย
- ฝรั่งเศส: 156 ราย
- ออสเตรเลีย: 154 ราย

hypothesis Microsoft Security